

Amendments to the Claims:

1. (Currently Amended) A microprocessor programmed to perform the steps of:

dividing a whole image that contains at least one region of flat content into a plurality of regions;

5 generating a signature including generating signature bits from each of the plurality of regions including the at least one region of flat content;

embedding the signature generated without subdividing the signature by spreading the signature bits of the signature across at least a portion of the image which is larger than one of the regions, such that the signature bits from all regions
10 can be extracted even if the at least one region of flat content has been replaced by tampering whereby the image is protected from tampering in the at least one region of flat content.

2. (Cancelled)

3. (Previously Presented) The microprocessor according to claim 1 wherein the signature is embedded as a watermark.

4. (Previously Presented) The microprocessor according to claim 3 wherein the watermark is a spread spectrum watermark.

5. (Previously Presented) The microprocessor according to claim 3 wherein the watermark is embedded according to a trade-off between a payload size of the image, a robustness of the watermark, and a visibility of the watermark.

6. (Previously Presented) The microprocessor according to claim 1 wherein each signature bit is embedded multiple times in different locations within the image.

7. (Previously Presented) The microprocessor according to claim 1 wherein spreading the signature bits including:

decomposing the signature bits to multiple areas or a single large area within the image such that information needs to be extracted from the multiple areas or the single large area within the image, in order to evaluate the original signature bits.

8-10. (Cancelled)

11. (Cancelled)

12. (Previously Presented) A non-transitory computer readable medium having a plurality of computer-executable instructions which instructs a microprocessor to authenticate images, the computer executable instructions comprising:

5 a first program module which generates instructions for a computer for dividing the images into regions, at least one of the regions including an area of flat content;

a second program module which generates instructions for a computer for generating a signature, the signature being generated by generating at least one signature bit from each of the regions; and

10 a third program module which generates instructions for a computer for embedding the signature in the images without subdividing the signature, such that the signature is spread across at least a portion of the image which is larger than one of the regions such that the area of flat content is protected from tampering.

13. (Cancelled)

14. (Currently Amended) A method of authenticating an audio video signal, the method comprising:

receiving at least one video image with a processor;

with the processor, dividing the video image into a plurality of regions
5 including at least one region of flat content and a plurality of regions with non-flat
content;

with the processor, generating at least one bit of a signature from each of
the regions including from the at least one region of flat content;

with the processor, embedding the signature only in the plurality of
10 regions with the non-flat content; and

subsequently with the same or a different processor, extracting the
signature bits from the plurality of regions with the non-flat content and, from the
extracted bits, determining if the at least one region of flat content has been subject to
tampering.

15. (Previously Presented) One or more processors programmed to
perform the method according to claim 14.